

01807.002407.



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)	
	:	Examiner: Not Yet Assigned
PATRICE ONNO ET AL.)	
	:	Group Art Unit: Not Yet Assigned
Application No.: 10/621,418)	
	:	
Filed: July 18, 2003)	
	:	
For: METHOD AND DEVICE FOR)	
TRANSFORMING A DIGITAL	:	
SIGNAL)	October 27, 2003

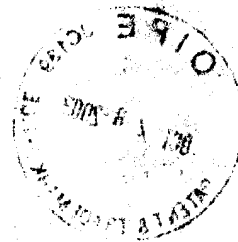
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF PRIORITY DOCUMENT

Sir:

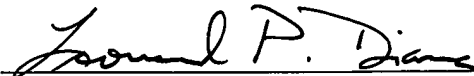
In support of Applicants' claim for priority under 35 U.S.C. § 119, enclosed is
a certified copy of the following French application:

0209134, filed July 18, 2002.



Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address given below.

Respectfully submitted,



Attorney for Applicants

Registration No. 28,286

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

NY_MAIN 380449v1



10/28/03

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 10 JUIL. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr





26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



REQUÊTE EN DÉLIVRANCE page 1/2

R1

Cet imprimé est à remplir lisiblement à l'encre noire


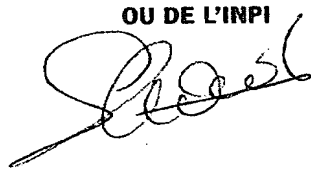
DB 540 W / 300301

REMISE DES PIÈCES DATE 18 JUL 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0209134 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE 18 JUL. 2002 PAR L'INPI		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE RINUY, SANTARELLI 14, avenue de la Grande Armée 75017 PARIS	
Vos références pour ce dossier (facultatif) BIF023190/MP/LJH			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> <i>ou demande de certificat d'utilité initiale</i>		N°	Date
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		N°	Date
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé et dispositif de transformation d'un signal numérique			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		CANON KABUSHIKI KAISHA	
Prénoms			
Forme juridique		Société de droit Japonais	
N° SIREN			
Code APE-NAF			
Rue		30-2, Shimomaruko 3-chome, Ohta-ku,	
Adresse		Tokyo,	
Code postal et ville			
Pays		JAPON	
Nationalité		JAPONAISE	
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			

Remplir impérativement la 2^{ème} page

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
REQUÊTE EN DÉLIVRANCE
 page 2/2

R2

REMISE DES PIÈCES DATE 18 JUIL 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0209134 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	DB 540 W / 300301
Vos références pour ce dossier : <i>(facultatif)</i>		BIF023190/MP/LJH	
6 MANDATAIRE			
Nom Prénom Cabinet ou Société		RINUY, SANTARELLI	
N °de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	14 AVENUE DE LA GRANDE ARMÉE	
	Code postal et ville	7 5 0 1 7 PARIS	
N° de téléphone <i>(facultatif)</i>		01 40 55 43 43	
N° de télécopie <i>(facultatif)</i>			
Adresse électronique <i>(facultatif)</i>			
7 INVENTEUR (S)			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en deux versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention <i>(joindre un avis de non-imposition)</i> <input type="checkbox"/> Requête antérieurement à ce dépôt <i>(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)</i>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)		VISA DE LA PRÉFECTURE OU DE L'INPI	
 Maxime PETIT N°00.0407 RINUY, SANTARELLI			

5

10 La présente invention concerne un procédé et un dispositif de transformation d'un signal numérique en vue de sa transmission, le signal étant décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée.

15 L'invention concerne également un procédé et un dispositif de transformation d'un signal numérique après réception de ce dernier.

L'invention s'applique notamment dans le domaine du traitement des images et, par exemple, dans le domaine du traitement d'images conformes à la norme JPEG2000.

20 Selon cette norme, un signal numérique d'image compressé possède une structure générale comportant des données d'en-tête constituant un en-tête principal et un corps qui comporte, sous forme compressée, des données représentatives de grandeurs physiques que sont les pixels et qui sont regroupées en blocs de données (connus en terminologie anglo-saxonne sous le
25 terme "code-blocks") ordonnés dans le signal.

Le corps du signal correspond au moins à une tuile qui représente de façon compressée une portion rectangulaire du signal d'image d'origine. Chaque tuile est formée de données d'en-tête de tuile et d'un corps de tuile contenant les blocs de données compressées correspondant à la tuile considérée.

30 Plus particulièrement, le corps de chaque tuile comporte des paquets de données qui sont chacun constitués de données d'en-tête de paquet et d'un corps de paquet.



Le corps de paquet contient à son tour plusieurs blocs de données compressées et les données d'en-tête du paquet contiennent notamment une liste de tous les blocs contenus dans le corps de paquet.

5 Chaque bloc de données compressées est une représentation compressée d'une portion rectangulaire élémentaire du signal d'image d'origine qui a été transformée, de manière connue, en sous-bandes de fréquence, par exemple, par une transformée en ondelettes discrète.

10 Il convient de noter que chaque bloc de données est compressé sur plusieurs couches de qualité et chaque couche de qualité d'un bloc se trouve dans un paquet distinct.

Chaque paquet de données d'un signal d'image compressé conforme à la norme JPEG2000 contient donc un ensemble de blocs de données compressées correspondant chacun à une tuile, une composante (exemple :
15 luminance ou chrominance), un niveau de résolution, une couche de qualité et une position ou localisation spatiale (connue en terminologie anglo-saxonne sous le terme "precinct") donnés.

Il est connu d'effectuer un brouillage ou cryptage de signaux numériques comme, par exemple, des images avant de transmettre ces signaux et ce, afin de s'assurer que des personnes non autorisées recevant ces signaux
20 ne pourront pas en exploiter le contenu.

Par ailleurs, d'après un document intitulé "Partial encryption compressed images and videos" de H. Cheng et X. Li, IEEE Transactions on Signal Processing, 48(8) pages 2439-2451, 2000, il est également connu d'effectuer un cryptage partiel de signaux d'images et de vidéos afin de réduire le
25 temps nécessaire aux opérations de cryptage et de décryptage.

La technique proposée prévoit de modifier l'unité de codage entropique du dispositif de compression, ce qui rend par là-même impossible l'utilisation d'un décodeur classique compatible avec la norme JPEG2000 pour effectuer les opérations de décompression du signal d'image.

30 Il est également connu du document EP 1033880 publié le 6 septembre 2000 au nom de Sharp KK une technique de cryptage de signaux d'images qui effectue notamment un mélange des données constitutives d'un signal d'image avant le codage entropique de ces données.

Là encore, la technique envisagée prévoit de traiter toute l'image et les données ainsi traitées sont ensuite codées de façon entropique, suivant un ordre prédéterminé qui n'est pas l'ordre naturel suivant lequel elles sont habituellement codées.

5 Cette technique est relativement compliquée à mettre en œuvre et induit en outre un temps de traitement relativement important.

10 La Demanderesse s'est également aperçue que les problèmes évoqués ci-dessus se posent également pour des signaux numériques qui ne sont pas des signaux d'image ni des signaux vidéo et qui peuvent, par exemple, être des signaux audio, voire des signaux issus de télécopieurs ou d'autres systèmes de communication.

15 La présente invention prévoit ainsi de remédier à au moins un des inconvénients précités en proposant un procédé et un dispositif de transformation d'un signal numérique qui soient particulièrement simples et efficaces.

20 La présente invention a ainsi pour objet un procédé de transformation d'un signal numérique en vue de sa transmission, le signal étant décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée, caractérisé en ce que le procédé comporte une étape de modification, parmi les données d'en-tête propres à au moins une zone du signal, de la partie des données d'en-tête qui est représentative de l'amplitude des données de la zone considérée.

25 Corrélativement, l'invention concerne également un dispositif de transformation d'un signal numérique en vue de sa transmission, le signal étant décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée, caractérisé en ce que le dispositif comporte des moyens de modification, parmi les données d'en-tête propres à au moins une zone du signal, de la partie des données d'en-tête qui est représentative de l'amplitude des données de la zone considérée.

30



Ainsi, en choisissant de modifier la partie des données d'en-tête propre à une zone du signal qui est représentative de l'amplitude des données de cette zone, on n'altère pas les données constitutives du signal et on ne modifie pas non plus la structure de ce dernier.

5 En outre, le cryptage proposé ici peut être opéré sur une portion ou zone sélectionnée du signal et non nécessairement sur tout le signal, ce qui réduit par là-même considérablement le temps consacré aux opérations de cryptage ainsi que la complexité de celles-ci.

10 De même, l'invention est particulièrement avantageuse dans la mesure où il est possible de sélectionner la ou les zones que l'on souhaite crypter.

 Le cryptage proposé selon l'invention est de préférence effectué lors des opérations de compression du signal numérique ou bien sur le signal numérique déjà compressé.

15 Plus particulièrement, les données numériques du signal étant des échantillons numériques représentatifs de grandeurs physiques, la partie des données d'en-tête représentative de l'amplitude des échantillons de la zone considérée fournit un nombre de plans de bits sur lesquels sont codées les amplitudes des échantillons à partir de la différence entre, d'une part, un nombre de plans de bits dit de référence, dépendant du signal et qui est déduit
20 d'informations présentes dans le signal et, d'autre part, un nombre de plans de bits nuls qui est contenu dans ladite partie des données d'en-tête.

 Dans ce contexte, il est ainsi, par exemple, prévu que l'étape de modification selon l'invention modifie le nombre de plans de bits nuls.

25 La modification d'un paramètre représentant le nombre de plans de bits nuls des échantillons de la zone considérée va induire, dans le signal qui sera transmis, une valeur erronée quant à l'amplitude de ces échantillons.

 Ainsi, au niveau du récepteur d'un tel signal, un décodeur classique sera capable de décoder le ou les paramètres modifiés selon l'invention mais le résultat de ce décodage se traduira par des données qui ne correspondent pas
30 aux données réelles avant leur cryptage.

 Dans le cas d'un signal d'image, l'image qui sera ainsi décompressée sera floue et distordue, rendant par là-même son exploitation impossible. Il convient de noter que, même si le contenu du signal peut malgré tout être

reconnu, la qualité de restitution de ce dernier est néanmoins largement dégradée par rapport à la qualité qui serait normalement obtenue en l'absence de cryptage.

5 Plus particulièrement, l'étape de modification selon l'invention prévoit d'augmenter le nombre de plans de bits nuls par rapport au nombre réel de plans de bits nuls des échantillons de la zone considérée.

De cette façon, à la réception du signal transformé selon l'invention, le nombre de plans de bits nuls des échantillons d'une zone a une certaine valeur qui se trouve être supérieure à la valeur réelle.

10 Par conséquent, lors des étapes de décompression du signal, le récepteur ne va prendre en compte les amplitudes des échantillons de la zone que sur un nombre de plans de bits réduit par rapport au nombre réel.

15 Ainsi, les amplitudes des échantillons obtenues après les opérations de décompression ne reflèteront pas la réalité des amplitudes des échantillons du signal d'origine avant cryptage.

Selon une caractéristique, l'étape de modification fait intervenir au moins une clé de transformation Ku.

Cette clé peut également tenir compte de la portion ou zone du signal qui doit être cryptée.

20 Ainsi, la transmission de cette clé au récepteur du signal indique à ce dernier la portion ou zone qui a été cryptée.

Selon une caractéristique, le procédé selon l'invention comporte une étape de génération d'une séquence pseudo-aléatoire à partir de la clé de transformation Ku.

25 Selon un autre aspect, l'invention concerne également un procédé de transformation d'un signal numérique décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée, caractérisé en ce que le procédé
30 comporte les étapes suivantes :

- réception du signal dont la partie des données d'en-tête représentative de l'amplitude des données d'au moins une zone a subi une modification avant la transmission dudit signal,

- modification inverse de cette partie modifiée des données d'en-tête afin de restituer ladite partie non modifiée des données d'en-tête du signal.

5 Corrélativement, l'invention concerne en outre un dispositif de transformation d'un signal numérique décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée, caractérisé en ce que le dispositif comporte :

10 - des moyens de réception du signal dont la partie des données d'en-tête représentative de l'amplitude des données d'au moins une zone a subi une modification avant la transmission dudit signal,

 - des moyens de modification inverse de cette partie modifiée des données d'en-tête afin de restituer ladite partie non modifiée des données d'en-tête du signal.

15 Ainsi, un récepteur d'un signal numérique transformé selon l'invention est capable de restituer la partie du signal qui a été modifiée par de simples opérations consistant à effectuer une modification inverse de celle appliquée, au niveau de l'émetteur, à la partie des données d'en-tête qui est représentative de l'amplitude des données d'au moins une zone du signal.

20 L'invention mise en œuvre dans un récepteur du signal transformé selon l'invention présente les mêmes avantages que ceux apportés par l'invention lorsqu'elle est mise en œuvre dans un émetteur du signal, à savoir la simplicité du cryptage / décryptage proposé, la rapidité avec laquelle il est possible de crypter / décrypter le signal puisque les données constitutives du signal sont préservées, de même que la conservation du taux de compression dans le signal crypté.

25 L'invention concerne également un appareil de communication comportant un dispositif de transformation d'un signal numérique, tel que brièvement exposé ci-dessus.

 Selon un autre aspect, l'invention vise aussi :

30 - un moyen de stockage d'informations lisible par un ordinateur ou un microprocesseur comportant des instructions de code d'un programme d'ordinateur pour l'exécution des étapes du procédé selon l'invention tel que celui exposé brièvement ci-dessus, et

- un moyen de stockage d'informations amovible, partiellement ou totalement, lisible par un ordinateur ou un microprocesseur comportant des instructions de code d'un programme d'ordinateur pour l'exécution des étapes du procédé selon l'invention tel que celui brièvement exposé ci-dessus.

5 Selon encore un autre aspect, l'invention vise un programme d'ordinateur chargeable dans un appareil programmable, comportant des séquences d'instructions ou portions de code logiciel pour mettre en œuvre des étapes du procédé de l'invention tel que brièvement exposé ci-dessus, lorsque ledit programme d'ordinateur est chargé et exécuté sur l'appareil programmable.

10 Les caractéristiques et avantages relatifs au dispositif de transformation d'un signal numérique, à l'appareil de communication comportant un tel dispositif, aux moyens de stockage d'informations et au programme d'ordinateur étant les mêmes que ceux exposés ci-dessus concernant le procédé selon l'invention, ils ne seront pas rappelés ici.

15 D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description qui va suivre, faite en référence aux dessins annexés, sur lesquels :

- la figure 1 est une représentation schématique d'une architecture possible de communication dans laquelle l'invention est mise en œuvre ;

20 - la figure 2 illustre de façon schématique un train binaire conforme à la norme JPEG2000 ;

- la figure 3a fournit une représentation en trois dimensions des amplitudes des échantillons d'un bloc de données suivant un nombre de plans de bits de référence ;

25 - la figure 3b est une représentation modifiée de la figure 3a après modification selon l'invention ;

- la figure 4 est une représentation de paquets de données d'une même résolution du train binaire de la figure 2 ;

30 - la figure 5 est un algorithme de transformation selon l'invention d'un signal numérique en vue de sa transmission ;

- la figure 6 est un algorithme de transformation selon l'invention d'un signal numérique après réception de celui-ci;

- la figure 7 est une représentation schématique d'un appareil programmable dans lequel l'invention est mise en œuvre.

5 L'invention concerne la transformation d'un signal numérique qui peut avantageusement être mise en œuvre entre deux appareils de communication, l'un émetteur, noté 10 sur la **figure 1** et l'autre récepteur, noté 12 sur cette même figure, par l'intermédiaire d'un réseau de communication 14.

Dans le contexte de l'invention, l'appareil de communication 10 dispose d'un signal numérique qu'il souhaite transmettre à l'appareil de communication distant 12 par l'intermédiaire du réseau 14.

10 Pour ce faire, l'appareil 10 va transformer (cryptage) avant la transmission le signal numérique qui sera, par exemple, compressé, afin de le rendre inexploitable dans l'hypothèse où il serait reçu par un destinataire non autorisé.

15 Dans le contexte de l'invention, l'appareil de communication 12 est récepteur d'un tel signal transformé et, en tant que destinataire autorisé, possède les moyens qui le rendent apte à effectuer sur le signal reçu une transformation inverse de celle qu'il a subi dans l'appareil 10.

Ceci permet donc d'effectuer un décryptage du signal dans l'appareil 12 afin qu'un utilisateur autorisé puisse exploiter ce signal.

20 L'invention trouve une application particulièrement intéressante dans le cadre des signaux d'image et, encore plus particulièrement, lorsque ceux-ci sont conformes à la norme JPEG2000.

25 On rappellera que, selon cette norme, un signal numérique d'image compressé comporte des données d'en-tête constituant un en-tête principal, des données d'en-tête de tuiles suivant lesquelles le signal est partitionné (une tuile représente, de façon compressée, une portion rectangulaire du signal d'image qui comporte toujours au moins une tuile) et, pour chaque tuile, un corps de tuile comportant des paquets de données qui sont chacun constitués de données d'en-tête de paquet et d'un corps de paquet.

30 Le corps de paquet contient à son tour plusieurs blocs de données compressées qui sont représentatives de grandeurs physiques que sont les pixels de l'image.

Les données d'en-tête de paquet contiennent notamment une liste de tous les blocs contenus dans le corps de paquet.

Chaque bloc de données compressées est une représentation compressée d'une portion rectangulaire élémentaire du signal d'image qui a été
5 décomposée, de manière connue, en sous-bandes de fréquence.

Il convient de noter que chaque bloc de données est compressé sur plusieurs couches de qualité et chaque couche de qualité d'un bloc se trouve dans un paquet distinct.

Par ailleurs, les tuiles précitées sont compressées de façon
10 indépendante.

Chaque paquet de données d'un signal d'image conforme à la norme JPEG2000 contient donc un ensemble de blocs de données compressées correspondant chacun à une tuile, une composante (par exemple : luminance ou chrominance), un niveau de résolution, une couche de qualité et une position ou
15 localisation spatiale (connue en terminologie anglo-saxonne sous le terme "precinct") donnés.

Comme représenté sur la **figure 2**, le train binaire d'un signal d'image conforme à la norme JPEG2000 comporte des données d'en-tête principal notées EN et des paquets de données $P(r,q)$, où r et q sont des entiers
20 représentant respectivement le niveau de résolution et la couche de qualité des paquets.

On notera que, par souci de simplification, pour l'exposé de l'invention il n'est pas nécessaire de tenir compte des autres paramètres que sont les tuiles, les composantes et les positions spatiales dans le signal.

Les données d'en-tête principal EN comportent notamment les informations suivantes, à savoir la taille de l'image, le nombre de tuiles formées dans cette image, le type de filtre utilisé pour la décomposition en sous-bandes de fréquence, le pas de quantification et des paramètres de codage comme, par
25 exemple, l'organisation du train binaire utilisée et le nombre de couches de
30 qualité.

Ces informations sont utiles lors des opérations de décompression effectuées sur le train binaire qui comporte des données compressées.



Les données d'en-tête principal contiennent également, de manière générale, les informations permettant d'obtenir le nombre de plans de bits dit de référence qui dépend du signal et de sa décomposition en sous-bandes de fréquence.

5 Plus particulièrement, le nombre de plans de bits de référence propre à une sous-bande de fréquence est déduit du nombre de bits sur lesquels le signal est codé, du nombre de niveaux de décompositions et de la sous-bande de fréquence considérée.

10 Sur la figure 2 les paquets de données sont organisés en couches de qualité : la première couche de qualité 1 correspond à une qualité donnée, par exemple, 0,01 bpp (bit par pixel), tandis que les couches de qualité suivantes ..., j, ..., N contiennent des données additionnelles et correspondent à des qualités supérieures.

15 On notera que la représentation du train binaire est alors dite progressive en qualité.

La **figure 3a** illustre de façon schématique la représentation en plans de bits des amplitudes des quatre pixels formant un bloc de données.

20 Comme représenté sur cette figure, chaque pixel ou échantillon numérique représentatif de la grandeur physique qu'est le pixel possède une amplitude traduite sous forme binaire qui est répartie sous la forme de 0 et de 1 dans les différents plans de bits représentés.

25 On notera que ce ne sont pas nécessairement des pixels d'un bloc de données dont les amplitudes sont représentées sous la forme de plans de bits à la figure 3a mais qu'il peut également s'agir d'échantillons numériques représentatifs de ces pixels et qui sont, par exemple, obtenus à partir de ces derniers par une décomposition en sous-bandes de fréquence.

On notera que le premier plan de bits noté 101 représente le plan de bits le moins significatif, les plans de bits suivants 102 ... 109 représentant respectivement les plans de bits de plus en plus significatifs.

30 Dans l'exemple considéré, les plans de bits 108 et 109 ne contiennent que des 0 et sont appelés plans de bits nuls. Conformément à la norme JPEG2000, dans les données d'en-tête de paquets du signal d'image, un

paramètre de codage est présent pour signaler le nombre de plans de bits nuls afin de ne pas effectuer un codage inutile des valeurs nulles.

Dans l'exemple considéré, ce paramètre de codage est égal à 2.

5 On notera que le nombre de plans de bits 101 à 109 de la figure 3a représente le nombre de plans de bits de référence évoqué plus haut, par exemple égal à 20, et ce nombre est la somme du nombre de plans de bits sur lesquelles sont codées les amplitudes des données du signal (101 à 107), par exemple égal à 18, et du nombre de plans de bits nuls (108 et 109) qui est, par exemple, égal à 2.

10 Ainsi, connaissant le nombre de plans de bits nuls d'après les données d'en-tête du paquet considéré et déduisant le nombre de plans de bits de référence de la sous-bande de fréquence considérée des données d'en-tête principal, on obtient aisément le nombre réel de plans de bits sur lesquels sont codées les amplitudes des données du signal.

15 Cette dernière information intéresse le récepteur du signal puisqu'elle lui permettra de restituer le signal tel qu'il était avant cryptage. Pour ce faire, le récepteur du signal devra savoir quelle zone a été cryptée pour aller chercher les informations pertinentes dans les données d'en-tête principal et dans les données d'en-tête du paquet concerné.

20 Le paramètre est ensuite codé de façon connue sous la forme d'un arbre d'identification (connu en terminologie anglo-saxonne sous le terme "tag-tree") dans les données d'en-tête de paquets.

Cette technique de codage est connue notamment de la norme JPEG2000 ISO/IEC15444-1 "JPEG2000 Image Coding System" Annexe B
25 Section B.10.

On notera que ce paramètre de codage apparaît uniquement lorsque le bloc de données concerné contribue pour la première fois à un paquet de données.

30 Il convient également de noter que la notion de codage qui est ici considérée est différente de celle prévue pour le codage entropique des données lors des opérations de compression du signal d'image.

Par souci de simplification, on ne mentionnera plus par la suite le fait que le paramètre est codé dans les données d'en-tête de paquets.

Sur la **figure 3b** on a représenté les plans de bits 101 à 109 de la figure 3a de façon décalée, après avoir inséré de façon artificielle deux plans de bits nuls supplémentaires 110 et 111.

5 Ainsi, vu du récepteur du signal transformé selon l'invention, le nombre de plans de bits de référence déduit des informations présentes dans les données d'en-tête principal étant toujours le même (20), le nombre modifié (4) de plans de bits nuls (108 à 111) qui est fourni par les données d'en-tête de paquet induira en erreur le récepteur non autorisé à recevoir ce signal.

10 Ce dernier déduira en effet de ce qui précède que le nombre de plans de bits sur lesquels sont codées les amplitudes des données du signal est de 16 (plans de bits 101 à 105) alors qu'il est en fait de 18 plans de bits.

15 Ainsi, lors des opérations de décompression du signal transformé, le récepteur non autorisé commencera par s'intéresser au premier plan de bit non nul, à savoir le plan de bit référencé 107 sur la figure 3b, qu'il considérera comme étant le cinquième plan de bits à partir de la référence faussée et, à partir de là, il prendra en compte uniquement les 15 plans de bits suivants pour arriver à un total de 20.

De ce fait, les plans de bits 101 et 102 ne seront pas pris en considération.

20 De plus, étant donné que l'on a inséré deux plans de bits nuls 110 et 111, le décalage induit au niveau des plans de bits entraîne, pour chaque plan de bits nuls inséré, une division par deux de l'amplitude des échantillons et la qualité du signal restitué sera donc dégradée.

25 Par ailleurs, il convient de noter que la dégradation constatée sur la qualité du signal restitué est accentuée par le fait que la modification apportée à chaque bloc de données varie d'un bloc à l'autre.

Sur la **figure 4**, on a représenté de façon plus détaillée que sur la figure 2 plusieurs paquets de données d'une même résolution.

30 Chaque paquet a été représenté sous la forme de données d'en-tête et d'un corps de paquet.

On a par exemple représenté dans les en-têtes des paquets 1, 2, 3 et N les paramètres qui fournissent, dans les données d'en-tête de paquet, le nombre de plans de bits nuls pour le bloc CB_i considéré, où $i = 1$ à 8.

Les paramètres sont ainsi notés BPN(CBi).

Comme indiqué plus haut, pour un bloc de données considéré, le paramètre fournissant le nombre de plans de bits nuls est inclus dans les données d'en-tête d'un paquet lorsque ce bloc contribue pour la première fois à ce paquet. Bien que ce bloc de données puisse ensuite contribuer à d'autres paquets de données, le paramètre précité ne sera pas inclus dans les données d'en-tête de ces autres paquets.

On notera que, dans le cadre de l'invention, le signal numérique auquel s'applique l'invention est décomposé en plusieurs zones qui contiennent chacune des données numériques et que le signal comprend des données d'en-tête qui sont propres à chaque zone.

Les zones considérées ici au sens de l'invention sont, par exemple, des blocs de données. Les données d'en-tête propres à chaque zone sont alors les données d'en-tête de paquet.

Il est également possible de considérer qu'une zone correspond à une tuile et que dans ce cas les données d'en-tête propres à la tuile sont les données d'en-tête de tuile.

Toutefois, une zone au sens de l'invention peut également correspondre, de façon plus générale, à une portion spatiale et/ou fréquentielle du signal.

Au sens de la présente invention, les données d'en-tête de paquet comportent une ou plusieurs parties représentatives chacune de l'amplitude des données d'une zone considérée, c'est-à-dire d'un bloc de données.

Dans l'exemple du paquet 1, les données du paquet 1 contiennent plus particulièrement des données d'en-tête propres à chaque bloc de données CB1, CB5 et CB7 comportant une partie, notée respectivement pour les blocs précités, BPN(CB1), BPN(CB5) et BPN(CB7), et qui est représentative de l'amplitude des données du bloc considéré.

La **figure 5** est un algorithme comportant différentes instructions ou portions de code correspondant à des étapes du procédé de transformation d'un signal numérique selon l'invention et qui est mis en œuvre dans l'appareil de communication 10 de la figure 1.



Un programme d'ordinateur noté "Prog 1" basé sur cet algorithme est stocké dans l'appareil représenté à la figure 7 et qui sera décrit ultérieurement.

5 Ce programme est stocké dans une mémoire morte et, à l'initialisation du système, est transféré dans une mémoire vive en vue de l'exécution du programme et donc de la mise en œuvre du procédé selon l'invention.

Au cours de l'exécution de cet algorithme, on effectue plus particulièrement le cryptage d'un signal numérique, par exemple, compressé et qui est ici un signal d'image.

10 Au cours d'une première étape notée E10, on effectue une décomposition en sous-bandes de fréquence d'un signal numérique d'image que l'on souhaite transmettre à l'appareil de communication 12 de la figure 1.

Plus particulièrement, au cours de cette étape on applique au signal, par exemple, une transformée en ondelettes (DWT).

15 On peut bien entendu appliquer une autre transformée telle que, par exemple, une transformée en cosinus discret (DCT).

Au cours de l'étape suivante E11, on effectue une quantification des coefficients issus de la décomposition en sous-bandes de fréquence du signal d'image.

20 Chaque sous-bande de fréquence est ensuite divisée en plusieurs blocs de données de taille rectangulaire.

L'algorithme de la figure 5 comporte ensuite une étape E12 de codage entropique des blocs de données obtenus à l'étape précédente.

25 Au cours de cette étape de codage entropique, chaque bloc est codé indépendamment et l'on mémorise pour chacun d'eux le nombre de plans de bits nuls que l'on trouve. Ainsi, dans l'exemple représenté à la figure 3a, ce nombre est égal à 2.

On notera par ailleurs qu'à la suite de la décomposition en sous-bandes de fréquence du signal d'image on connaît, pour chaque sous-bande, le nombre de plans de bits de référence.

30 Cette information présente dans les données d'en-tête principal du signal sera transmise avec le signal à l'appareil de communication 12 de la figure 1 qui pourra alors, à l'aide de cette dernière et de l'information sur la portion ou zone du signal qui a été cryptée, retrouver le nombre de plans de bits nuls de

chaque bloc de données du signal d'image d'origine et donc procéder à un décryptage de ce signal.

5 L'algorithme de la figure 5 comporte en outre une étape E13 au cours de laquelle on procède à une allocation de débit, en ce sens que les données ou échantillons contenus dans les différents blocs de données sont répartis dans les paquets de données.

Au cours de cette étape, on crée de façon provisoire les données d'en-tête de paquet et, de façon définitive, le corps de ces paquets.

10 Il convient de noter que les étapes précitées correspondent aux étapes qui sont effectuées de manière conventionnelle dans un codeur conforme à la norme JPEG2000.

Au cours de l'étape suivante E14, l'algorithme de la figure 5 prévoit la génération d'une séquence pseudo-aléatoire à partir d'une clé secrète de transformation notée Ku.

15 On notera que la clé de transformation dépend des caractéristiques de l'appareil émetteur du signal ainsi que de la ou des zones du signal d'image à crypter (résolution, zone spatiale).

La clé de transformation secrète Ku est générée au cours d'une étape E15.

20 La clé de transformation secrète est utilisée comme "graine" dans le générateur de séquence pseudo-aléatoire. Lors de l'exécution de l'étape E14, la séquence pseudo-aléatoire générée prendra des valeurs entières entre 0 et M, où M est un entier servant de paramètre de modulation.

25 Ce paramètre de modulation est connu à la fois de l'appareil émetteur (appareil 10 de la figure 1) et de l'appareil récepteur (appareil 12 de la figure 1). On notera que ce paramètre pourrait également être codé sur un nombre défini de bits dans la clé de transformation secrète qui sera identique pour l'appareil émetteur et l'appareil récepteur.

30 La séquence pseudo-aléatoire générée a une longueur égale au nombre de blocs de données concernés par la transformation selon l'invention.

Ces blocs de données constituent, dans l'exemple de réalisation décrit, des zones au sens de la présente invention.



Comme représenté sur la figure 5, l'algorithme comporte une étape E16 au cours de laquelle les informations de taille de la portion ou zone du signal à crypter (X, Y, W, H) ainsi que le nombre N de résolutions sont déterminés.

5 Ces informations sont, par exemple, sélectionnées par l'utilisateur de l'appareil de communication émetteur.

On notera que ces informations peuvent être soit transmises de façon sécurisée à l'appareil de communication récepteur de façon indépendante, soit incluses dans la clé de transformation secrète Ku qui sera transmise à l'étape E21, en utilisant un nombre de bits fourni par la taille du signal d'image et le nombre de niveaux de décomposition comme indiqué ci-après. Les informations de taille de la partie du signal à brouiller et le nombre N de résolutions sont codés de la façon suivante :

15 X codé sur $\log_2(\text{largeur de l'image})$ bits
 Y codé sur $\log_2(\text{hauteur de l'image})$ bits
 W codé sur $\log_2(\text{largeur de l'image})$ bits
 H codé sur $\log_2(\text{hauteur de l'image})$ bits
 N codé sur $\log_2(\text{nombre de niveaux de décomposition})$ bits

20 Exemple : soit une image de largeur 2560 et de hauteur 5420 codée sur 6 niveaux de résolutions où la zone de brouillage se positionne en X=350 et en Y=400 avec une largeur de 2000 et une hauteur de 1500.

25 X sera alors codé sur $\log_2(2560)$, soit 11 bits
 Y sera alors codé sur $\log_2(5420)$, soit 12 bits
 W sera alors codé sur $\log_2(2560)$, soit 11 bits
 H sera alors codé sur $\log_2(5420)$, soit 12 bits
 N sera alors codé sur $\log_2(6)$, soit 3 bits.

La clé de transformation secrète Ku contiendra ainsi 49 bits pour spécifier la partie du signal d'image qui va être cryptée ainsi que les résolutions concernées.

30 En outre, la clé contiendra des bits supplémentaires, par exemple 128 bits, pour la génération de la séquence pseudo-aléatoire.

La portion du signal d'image destinée à être cryptée est définie au niveau du signal d'image à pleine résolution.

Cette portion du signal contient plusieurs blocs de données qui sont ici les zones au sens de la présente invention et que l'on doit crypter dans les différentes résolutions.

5 Afin de déterminer les blocs de données contenus dans la portion du signal à crypter, on projette cette portion du signal dans les différentes sous-bandes de fréquence obtenues à l'étape E10 de l'algorithme (étape E17).

10 Au cours de cette étape E17, les blocs de données des résolutions concernées et qui sont inclus dans la portion du signal projetée dans les différentes sous-bandes de fréquence fournissent une liste de blocs de données LCB correspondant à la portion du signal à crypter.

15 L'algorithme comporte une étape E18 au cours de laquelle on modifie, parmi les données d'en-tête des paquets de données contenant les contributions des blocs de données de la liste LCB, les parties de ces données d'en-tête qui sont représentatives de l'amplitude des données contenues dans les blocs de données considérés.

Cette modification est effectuée en utilisant la séquence pseudo-aléatoire contenant les valeurs de 0 à M et qui a été générée à l'étape E14.

20 Plus particulièrement, au cours de l'étape E18, on modifie le paramètre indiquant le nombre de plans de bits nuls pour les blocs de données présents dans la liste LCB, c'est-à-dire les blocs qui sont inclus dans la partie du signal à crypter et dans les résolutions concernées.

On notera que l'on peut effectuer un cryptage uniquement sur une résolution du signal.

25 Comme représenté sur la figure 4, les paramètres sur lesquels portent les modifications dans les données d'en-tête de paquet sont ceux notés BPN(CBi), avec $i = 1$ à 8 dans l'exemple de réalisation considéré.

On notera que les blocs de données seront traités dans un ordre particulier à savoir, par exemple, en commençant par les blocs contribuant à la première résolution qui correspond à la définition du signal d'image la plus faible.

30 Les blocs de données contribuant à une résolution donnée seront traités suivant un ordre de parcours naturel ligne par ligne et de haut en bas.

Cet ordre de parcours naturel est appelé en terminologie anglo-saxonne "raster scan".



La modification du paramètre BPN fournissant le nombre de plans de bits nuls du bloc de données $CB(i)$ appartenant à la liste des blocs LCB est effectuée de la façon suivante :

$$BPN'(CB_i) = [BPN(CB_i) + AL(i)], \text{ où } AL(i) \in [0, M]$$

5 Il convient de noter que la valeur du paramètre de modulation M est choisie de telle façon que la valeur modifiée du nombre de plans de bits nuls $BPN'(CB_i)$ n'excède pas le nombre de plans de bits de référence.

On notera que la modification apportée au nombre de plans de bits nuls des amplitudes des échantillons ou données de chaque bloc de données
10 consiste, par exemple, à faire passer le paramètre BPN de la valeur 2 dans l'exemple de la figure 3a à la valeur 4 dans l'exemple de la figure 3b.

On notera que l'on peut modifier de façon différente pour chaque bloc de données le nombre de plans de bits nuls les amplitudes des échantillons ou données du bloc considéré.

15 Ceci fournit un cryptage encore plus efficace que si la même modification est apportée pour chaque bloc car on crée ainsi des hétérogénéités dans le signal crypté.

De façon générale, les valeurs BPN des blocs sélectionnés sont modifiées de façon indépendante les unes des autres.

20 Cependant, à titre de variante, il est également possible de modifier la valeur $BPN(CB_i)$ en prenant en compte, par exemple, les valeurs BPN des blocs précédents dans l'ordre de parcours naturel du train binaire.

A l'issue de l'étape E18 de l'algorithme de la figure 5, les valeurs des paramètres fournissant le nombre de plans de bits nuls pour les blocs de
25 données considérés correspondant aux paquets 1, 2, 3 et N de la figure 4 sont alors modifiées pour prendre en compte les nouvelles valeurs des paramètres pour les blocs de données considérés.

On notera que l'invention permet avantageusement de ne pas toucher aux données elles-mêmes qui sont dans les corps des paquets.

30 La transformation du signal selon l'invention est donc plus simple et plus rapide que les méthodes proposées dans l'art antérieur. En outre, la transformation envisagée selon l'invention est très souple dans la mesure où elle peut être effectuée sur des blocs de données ou, plus généralement, des

portions ou zones du signal (par exemple des tuiles dans le cas d'un signal d'image JPEG2000) qui sont judicieusement choisies.

Ainsi, l'utilisateur peut par exemple sélectionner, comme on l'a vu précédemment, une portion ou zone spatiale du signal d'image afin de la crypter.

5 Par ailleurs, lorsqu'un signal comporte un nombre N de résolutions, il est possible d'effectuer un cryptage des résolutions N à k , tandis que les résolutions les plus basses (résolutions $(k-1)$ à 1) ne sont pas cryptées.

10 Au cours de l'étape E19, l'algorithme de la figure 5 prévoit d'effectuer un codage des données d'en-tête de paquet sous la forme d'un arbre d'identification ("tag-tree"), comme spécifié dans la norme JPEG2000 mentionnée plus haut.

Ainsi, les nouvelles valeurs des paramètres $BPN'(CBI)$ sont les valeurs nouvellement codées.

15 Au cours de l'étape suivante E20, on génère le signal numérique transformé incluant les différentes données d'en-tête (données d'en-tête principal et données d'en-tête de tuiles), ainsi que tous les paquets de données comprenant plus particulièrement les paquets de données non modifiés et les paquets modifiés.

20 Parmi les paquets modifiés, on trouve dans le signal transformé, pour chaque paquet, les données d'en-tête modifiées et le corps du paquet qui, lui, n'a pas été modifié.

25 Dans l'exemple de réalisation où le signal d'image est conforme à la norme JPEG2000, le signal d'image crypté généré à l'étape E20 est conforme à la syntaxe de description de la norme JPEG2000, mais il ne pourra pas être décodé de façon intelligible dans un appareil récepteur non autorisé, dans la mesure où le signal a été brouillé avant sa transmission.

Au cours de l'étape suivante E21, le signal d'image transformé (crypté) est transmis sur le réseau 14 de la figure 1 avec, par exemple, la clé K_u qui porte en elle-même les informations sur la ou les zones cryptées.

30 L'algorithme de la **figure 6** comporte différentes instructions aux portions de code correspondant à des étapes du procédé de transformation inverse selon l'invention et qui est mis en œuvre dans un appareil de



communication récepteur d'un signal transformé, tel que l'appareil de communication 12 de la figure 1.

Un programme d'ordinateur noté "Prog 2" basé sur cet algorithme est stocké dans l'appareil de communication de la figure 7 qui sera décrit ultérieurement.

L'exécution de ce programme d'ordinateur permet de mettre en œuvre le procédé selon l'invention dans l'appareil de communication récepteur d'un signal transformé.

L'algorithme de la figure 6 comporte une première étape E29 au cours de laquelle on procède à la réception du signal transformé (crypté) provenant de l'appareil 10 de la figure 1.

L'étape suivante E30 prévoit une analyse du flux binaire constituant le signal d'image crypté reçu par l'appareil exécutant cet algorithme.

Plus particulièrement, on extrait de ce flux binaire les paquets de données du signal d'image crypté, ainsi que la taille du signal d'image fourni par les données d'en-tête principal.

Au cours de l'étape suivante E31, les données d'en-tête des paquets de données sont décodées de façon inverse du codage prévu à l'étape E19 de l'algorithme de la figure 5.

Au cours de l'étape suivante E32, on génère la séquence pseudo-aléatoire à partir de la clé de transformation secrète K_u reçue de l'appareil émetteur, de façon identique à ce qui a été décrit en référence à la figure 5.

On notera que la clé secrète de transformation K_u est transmise de l'appareil de communication émetteur (appareil 10 de la figure 1) vers l'appareil de communication récepteur (appareil de communication 12) par des moyens sécurisés connus de l'homme de l'art.

Au cours de l'étape suivante E33, la clé de transformation K_u permet de déterminer la portion ou zone du signal d'image qui a été cryptée et le nombre de résolutions concernées.

On peut en effet, grâce à la taille du signal d'image obtenue à l'étape E30 et à la clé de transformation, retrouver la liste des blocs de données LCB cryptés dans les différentes résolutions.

Il convient de noter que l'on entend par bloc de données cryptées le bloc de données pour lesquelles une partie des données d'en-tête des paquets auxquels contribuent ces blocs ont été modifiées au sens de la présente invention, comme on l'a vu précédemment lors de la description de l'algorithme de la figure 5.

Cette liste des blocs est fournie à l'étape E34 de l'algorithme de la figure 6.

Au cours de l'étape suivante E35, on effectue sur les parties appropriées des données d'en-tête de paquet qui ont été modifiées dans l'appareil émetteur, une modification inverse de celle adoptée à la figure 5.

Plus particulièrement, on modifie les nombres de plans de bits nuls des échantillons ou données des différents blocs de données de la liste LCB précitée selon la formule suivante :

$$\text{BPN}(\text{CBi}) = (\text{BPN}'(\text{CBi}) - \text{AL}(i)),$$

où $\text{BPN}'(\text{CBi})$ est le paramètre fournissant le nombre de plans de bits nuls codé dans les données d'en-tête de paquet pour le bloc de données CBi considéré.

$\text{AL}(i)$ est la valeur de la séquence pseudo-aléatoire et $\text{BPN}(\text{CBi})$ est le paramètre fournissant le nombre de plans de bits nuls décrypté qui correspond ainsi à la valeur initiale avant cryptage.

A l'issue de cette étape, tous les paquets de données dont une partie des données d'en-tête a été modifiée lors du processus de cryptage prennent à nouveau les valeurs initiales du nombre de plans de bits nuls pour les blocs de données considérés, valeurs qu'ils avaient avant le cryptage.

Ainsi, le nombre de plans de bits nuls des données ou échantillons du bloc de données représenté à la figure 3b est ramené à la valeur représentée à la figure 3a, à savoir 2.

Au cours de l'étape suivante E36, on effectue un décodage entropique des différents blocs de données du signal d'image (étape inverse de l'étape E12 de la figure 5).

Au cours des étapes E37 et E38, on effectue respectivement les opérations de déquantification et de transformation inverse qui correspondent respectivement aux opérations inverses de celles effectuées aux étapes E11 et E10 de l'algorithme de la figure 5.



On obtient ainsi, à l'issue de l'étape E38, l'image originale reconstruite qui était présente avant la transformation selon l'invention appliquée, dans l'émetteur, grâce à l'algorithme de la figure 5.

5 A titre de variante, on peut crypter différentes résolutions d'un signal numérique avec une clé de transformation secrète pour chaque résolution afin de mieux tenir compte des résolutions et des données concernées dans chacune des résolutions.

10 Afin de ne pas avoir à gérer un nombre de clés égal au nombre de résolutions considérées, on peut utiliser une première clé et déduire les autres clés de la première en faisant appel, par exemple, à des fonctions de hachage.

De telles fonctions sont par exemple fournies ci-dessous :

$K2 = \text{Hash}(K1)$

$K3 = \text{Hash}(K2) = \text{Hash}(\text{Hash}(K1))$

$K4 = \text{Hash}(K3) = \text{Hash}(\text{Hash}(K2)) = \text{Hash}(\text{Hash}(\text{Hash}(K1)))$

15 Comme on vient de le voir lors de la description faite en référence aux figures 5 et 6, la transformation envisagée par l'invention, qu'il s'agisse du cryptage au niveau de l'émetteur ou du décryptage au niveau du récepteur, ne remet pas en question les opérations de compression et de décompression conventionnelles respectives du signal numérique.

20 On peut donc parfaitement intégrer l'invention à un système faisant intervenir un codeur et un décodeur conventionnels, ce qui ne remet pas en cause tout le processus de traitement d'un signal avant sa transmission et de traitement du signal une fois reçu.

25 Par ailleurs, dans la mesure où l'on peut effectuer un cryptage des niveaux de résolution les plus fins d'un signal tout en laissant les niveaux de résolution les plus bas non cryptés, on peut ainsi en quelque sorte contrôler l'accès aux résolutions correspondant aux définitions les plus fines du signal.

En référence à la **figure 7**, est décrit un exemple d'appareil de communication programmable mettant en œuvre l'invention.

30 Chacun des appareils de communication de la figure 1 est, par exemple, identique à l'appareil de la figure 7 et possède les moyens qui le rendent apte à la mise en œuvre de l'invention.

L'appareil de la figure 7 comprend un dispositif de transformation (cryptage ou décryptage) d'un signal numérique de l'invention selon que l'appareil est l'appareil 10 ou 12 de la figure 1.

5 Selon le mode de réalisation choisi et représenté à la figure 7, un appareil mettant en œuvre l'invention est par exemple un micro-ordinateur 200 ou une station de travail connecté à différents périphériques tels que, par exemple une caméra numérique 201 (ou un scanner, ou tout moyen d'acquisition ou de stockage d'image) reliée à une carte graphique et fournissant à l'appareil des données numériques.

10 L'appareil 200 comporte un bus de communication 202 auquel sont reliés :

- une unité centrale de traitement 203 (microprocesseur),
- une mémoire morte 204, pouvant comporter les programmes d'ordinateur "Prog1" et "Prog2",
- 15 - une mémoire vive 206 comportant des registres 207 adaptés à enregistrer des variables et paramètres créés et modifiés au cours de l'exécution des programmes précités, notamment, X, Y, W, H, AL (i), BPN (CBi), BPN'(i) mentionnés en référence aux figures précédentes, et les paquets de données traités au cours de l'exécution des différents algorithmes précédents.
- 20 - un écran 208 permettant de visualiser des données et/ou de servir d'interface graphique avec l'utilisateur qui pourra interagir avec les programmes selon l'invention, à l'aide d'un clavier 210 ou de tout autre moyen tel qu'un dispositif de pointage, comme par exemple une souris 211 ou un crayon optique,
- un disque dur 212 pouvant comporter les programmes "Prog1" et
- 25 "Prog2" précités,
- un lecteur de disquette 214 adapté à recevoir une disquette 216 et à y lire ou à y écrire des données numériques traitées ou à traiter selon l'invention,
- une interface de communication 218 reliée à un réseau de
- 30 communication distribué 220, par exemple le réseau Internet, l'interface étant apte à transmettre et à recevoir des données numériques.

Dans le cas de données audio, l'appareil comprend en outre une carte d'entrée/sortie (non représentée) reliée à un microphone 222.



Le bus de communication permet la communication et l'interopérabilité entre les différents éléments inclus dans le micro-ordinateur 200 ou reliés à lui. La représentation du bus n'est pas limitative et, notamment, l'unité centrale est susceptible de communiquer des instructions à tout élément du micro-ordinateur 200 directement ou par l'intermédiaire d'un autre élément du micro-ordinateur 200.

Le code exécutable de chaque programme permettant à l'appareil programmable de mettre en œuvre les processus des figures 5 et 6 selon l'invention, peut être stocké, par exemple, dans le disque dur 212 ou en mémoire morte 204 comme représenté sur la figure 7.

Selon une variante, la disquette 216, peut contenir des données ainsi que le code exécutable des programmes précités qui, une fois lu par l'appareil 200, sera stocké dans le disque dur 212.

En seconde variante, le code exécutable des programmes pourra être reçu par l'intermédiaire du réseau de communication 220, via l'interface 218, pour être stocké de façon identique à celle décrite précédemment.

Les disquettes peuvent être remplacées par tout support d'information tel que, par exemple, un disque compact (CD-ROM) ou une carte mémoire. De manière générale, un moyen de stockage d'information, lisible par un ordinateur ou par un microprocesseur, intégré ou non à l'appareil, éventuellement amovible, est adapté à mémoriser un ou plusieurs programmes dont l'exécution permet la mise en œuvre du procédé selon l'invention.

De manière plus générale, le ou les programmes pourront être chargés dans un des moyens de stockage de l'appareil 200 avant d'être exécutés.

L'unité centrale 203 va commander et diriger l'exécution des instructions ou portions de code logiciel du ou des programmes selon l'invention, instructions qui sont stockées dans le disque dur 212 ou dans la mémoire morte 204 ou bien dans les autres éléments de stockage précités. Lors de la mise sous tension, le ou les programmes qui sont stockés dans une mémoire non volatile, par exemple le disque dur 212 ou la mémoire morte 204, sont transférés dans la mémoire vive 206 (RAM) qui contiendra alors le code exécutable du ou des

programmes selon l'invention, ainsi que des registres pour mémoriser les variables et paramètres nécessaires à la mise en œuvre de l'invention.

Il convient de noter que l'appareil de communication comportant le dispositif selon l'invention peut également être un appareil programmé.

5

Cet appareil contient alors le code du ou des programmes informatiques par exemple figé dans un circuit intégré à application spécifique (ASIC).

REVENDEICATIONS

1. Procédé de transformation d'un signal numérique en vue de sa transmission, le signal étant décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée, caractérisé en ce que le procédé comporte une étape de modification (E18), parmi les données d'en-tête propres à au moins une zone du signal, de la partie des données d'en-tête qui est représentative de l'amplitude des données de la zone considérée.

2. Procédé selon la revendication 1, caractérisé en ce que les données numériques du signal étant des échantillons numériques représentatifs de grandeurs physiques, la partie des données d'en-tête représentative de l'amplitude des échantillons de la zone considérée fournit un nombre de plans de bits sur lesquels sont codées les amplitudes des échantillons à partir de la différence entre, d'une part, un nombre de plans de bits dit de référence, dépendant du signal et qui est déduit d'informations présentes dans le signal et, d'autre part, un nombre de plans de bits nuls qui est contenu dans ladite partie des données d'en-tête.

3. Procédé selon la revendication 2, caractérisé en ce que l'étape de modification prévoit de modifier le nombre de plans de bits nuls.

4. Procédé selon la revendication 3, caractérisé en ce que l'étape de modification prévoit d'augmenter le nombre de plans de bits nuls.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que l'étape de modification fait intervenir au moins une clé de transformation Ku.

6. Procédé selon la revendication 5, caractérisé en ce que la clé de transformation Ku dépend de ladite au moins une zone considérée.

7. Procédé selon la revendication 5 ou 6, caractérisé en ce que l'étape de modification fait notamment intervenir la génération (E14) d'une séquence pseudo-aléatoire à partir de la clé de transformation Ku.

8. Procédé selon l'une des revendications 5 à 7, caractérisé en ce qu'il comporte une étape de transmission de la clé de transformation Ku.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce qu'il comporte une étape de transmission du signal ainsi transformé.

10. Procédé de transformation d'un signal numérique décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée, caractérisé en ce que le procédé comporte les étapes suivantes :

- réception (E29) du signal dont la partie des données d'en-tête représentative de l'amplitude des données d'au moins une zone a subi une modification avant la transmission dudit signal,

- modification inverse (E35) de cette partie modifiée des données d'en-tête afin de restituer ladite partie non modifiée des données d'en-tête du signal.

11. Procédé selon la revendication 10, caractérisé en ce que les données numériques du signal étant des échantillons numériques représentatifs de grandeurs physiques, la partie des données d'en-tête représentative de l'amplitude des échantillons de la zone considérée fournit un nombre modifié de plans de bits sur lesquels sont codées les amplitudes des échantillons à partir de la différence entre, d'une part, un nombre de plans de bits dit de référence, dépendant du signal et qui est déduit d'informations présentes dans le signal et, d'autre part, un nombre modifié de plans de bits nuls qui est contenu dans ladite partie des données d'en-tête.

12. Procédé selon la revendication 11, caractérisé en ce que l'étape de modification inverse prévoit de modifier le nombre modifié de plans de bits nuls.

13. Procédé selon la revendication 12, caractérisé en ce que l'étape de modification inverse prévoit de diminuer le nombre modifié de plans de bits nuls.

14. Procédé selon l'une des revendications 10 à 13, caractérisé en ce que l'étape de modification inverse fait intervenir au moins une clé de transformation Ku.

15. Procédé selon la revendication 14 caractérisé en ce que la clé de transformation Ku dépend de ladite au moins une zone considérée.

16. Procédé selon la revendication 14 ou 15, caractérisé en ce que l'étape de modification inverse fait notamment intervenir la génération d'une séquence pseudo-aléatoire à partir de la clé de transformation Ku.

17. Procédé selon l'une des revendications 14 à 16, caractérisé en ce qu'il comporte une étape préalable de réception de la clé de transformation Ku.



18. Dispositif de transformation d'un signal numérique en vue de sa transmission, le signal étant décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée, caractérisé en ce que le dispositif comporte des
5 moyens de modification, parmi les données d'en-tête propres à au moins une zone du signal, de la partie des données d'en-tête qui est représentative de l'amplitude des données de la zone considérée.

19. Dispositif selon la revendication 18, caractérisé en ce que les
10 données numériques du signal étant des échantillons numériques représentatifs de grandeurs physiques, la partie des données d'en-tête représentative de l'amplitude des échantillons de la zone considérée fournit un nombre de plans de bits sur lesquels sont codées les amplitudes des échantillons à partir de la différence entre,
15 d'une part, un nombre de plans de bits dit de référence, dépendant du signal et qui est déduit d'informations présentes dans le signal et, d'autre part, un nombre de plans de bits nuls qui est contenu dans ladite partie des données d'en-tête.

20. Dispositif selon la revendication 19, caractérisé en ce que les moyens de modification modifient le nombre de plans de bits nuls.

21. Dispositif selon la revendication 20, caractérisé en ce que les moyens
20 de modification augmentent le nombre de plans de bits nuls.

22. Dispositif selon l'une des revendications 18 à 21, caractérisé en ce que les moyens de modification font intervenir au moins une clé de transformation Ku.

23. Dispositif selon la revendication 22, caractérisé en ce que la clé de
25 transformation Ku dépend de ladite au moins une zone considérée.

24. Dispositif selon la revendication 20 ou 21, caractérisé en ce qu'il comporte des moyens de génération d'une séquence pseudo-aléatoire à partir de la clé de transformation Ku.

25. Dispositif selon l'une des revendications 22 à 24, caractérisé en ce
30 qu'il comporte des moyens de transmission de la clé de transformation Ku.

26. Dispositif selon l'une des revendications 18 à 25, caractérisé en ce qu'il comporte des moyens de transmission du signal ainsi transformé.

27. Dispositif de transformation d'un signal numérique décomposé en plusieurs zones contenant chacune des données numériques, le signal comprenant des données d'en-tête propres à chaque zone et qui comportent au moins une partie représentative de l'amplitude des données de la zone considérée, caractérisé en ce que le dispositif comporte :

- des moyens de réception du signal dont la partie des données d'en-tête représentative de l'amplitude des données d'au moins une zone a subi une modification avant la transmission dudit signal,

- des moyens de modification inverse de cette partie modifiée des données d'en-tête afin de restituer ladite partie non modifiée des données d'en-tête du signal.

28. Appareil de communication, caractérisé en ce qu'il comporte un dispositif de transformation d'un signal numérique selon l'une des revendications 18 à 26.

29. Appareil de communication, caractérisé en ce qu'il comporte un dispositif de transformation d'un signal numérique selon la revendication 27.

30. Moyen de stockage d'informations lisible par un ordinateur ou un microprocesseur comportant des instructions de code d'un programme d'ordinateur pour l'exécution des étapes du procédé de transformation d'un signal numérique selon l'une des revendications 1 à 9.

31. Moyen de stockage d'informations lisible par un ordinateur ou un microprocesseur comportant des instructions de code d'un programme d'ordinateur pour l'exécution des étapes du procédé de transformation d'un signal numérique selon l'une des revendications 10 à 17.

32. Moyen de stockage d'informations amovible, partiellement ou totalement lisible par un ordinateur ou un microprocesseur comportant des instructions de code d'un programme d'ordinateur pour l'exécution des étapes du procédé de transformation d'un signal numérique selon l'une des revendications 1 à 9.

33. Moyen de stockage d'informations amovible, partiellement ou totalement lisible par un ordinateur ou un microprocesseur comportant des instructions de code d'un programme d'ordinateur pour l'exécution des étapes du



procédé de transformation d'un signal numérique selon l'une des revendications 10 à 17.

5 34. Programme d'ordinateur chargeable dans un appareil programmable, caractérisé en ce qu'il comporte des séquences d'instructions ou des portions de code logiciel pour mettre en œuvre les étapes du procédé de transformation d'un signal numérique selon l'une des revendications 1 à 9, lorsque ce programme d'ordinateur est chargé et exécuté par l'appareil programmable.

10 35. Programme d'ordinateur chargeable dans un appareil programmable, caractérisé en ce qu'il comporte des séquences d'instructions ou des portions de code logiciel pour mettre en œuvre les étapes du procédé de transformation d'un signal numérique selon l'une des revendications 10 à 17, lorsque ce programme d'ordinateur est chargé et exécuté par l'appareil programmable.

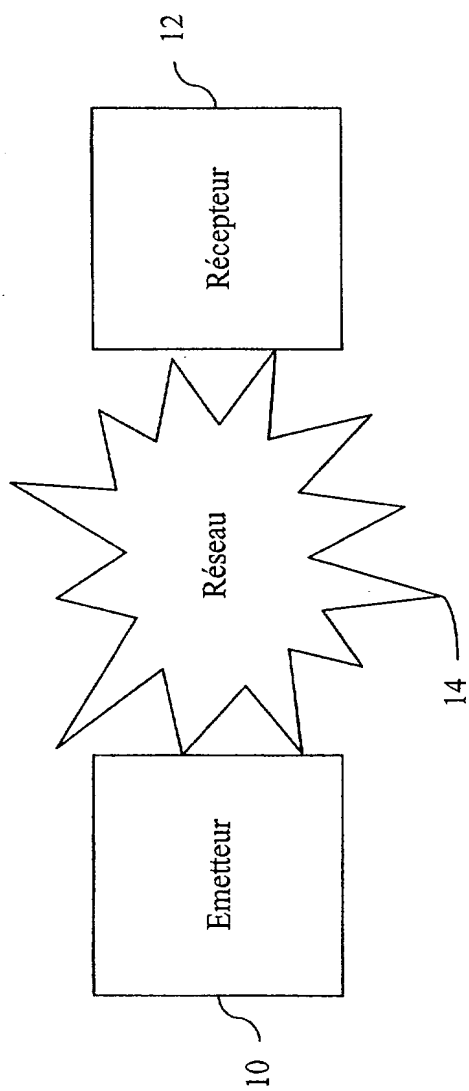


Fig. 1

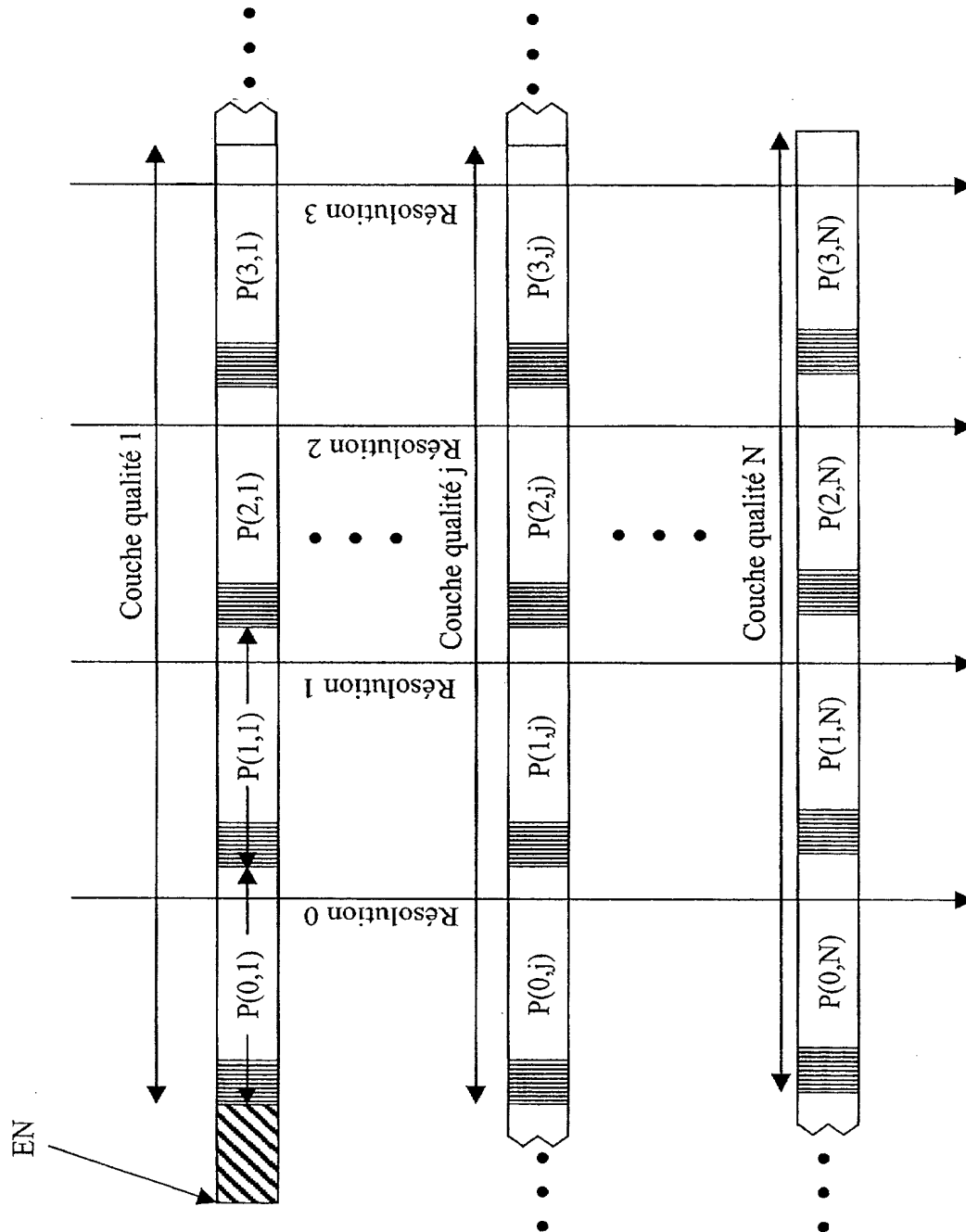


Fig. 2

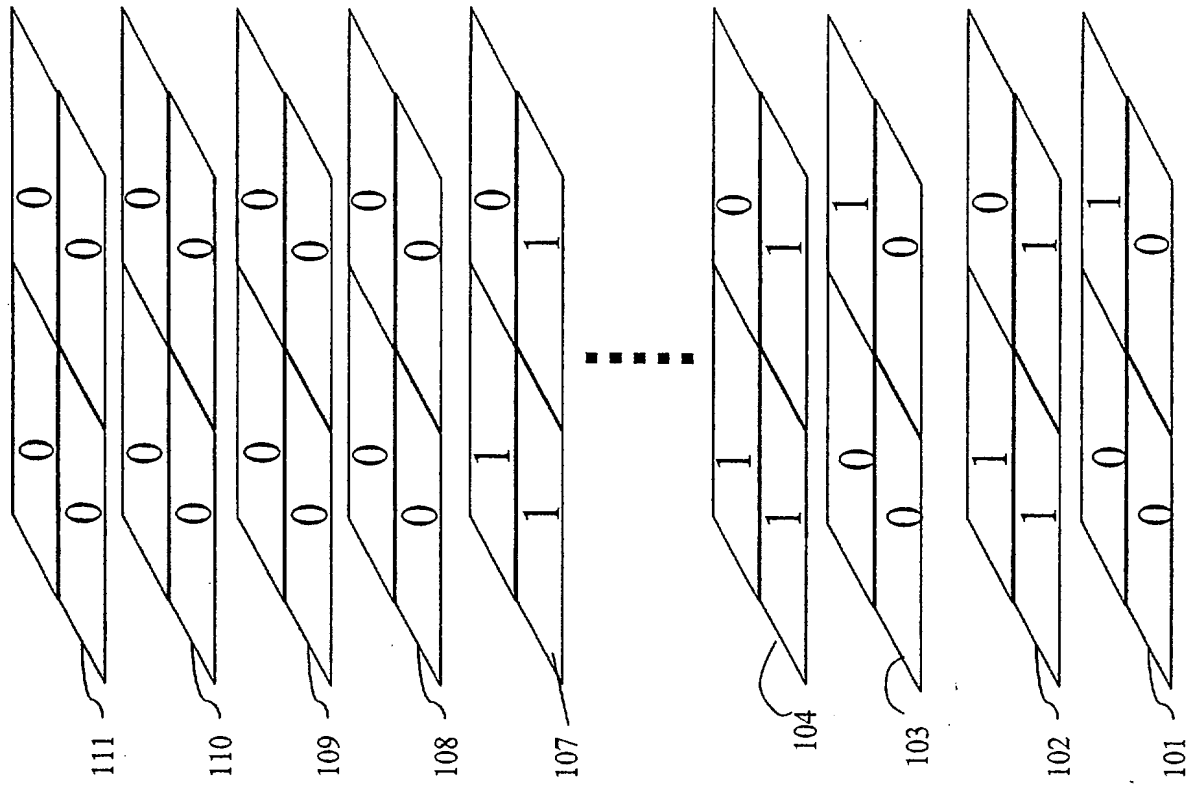


Fig. 3a

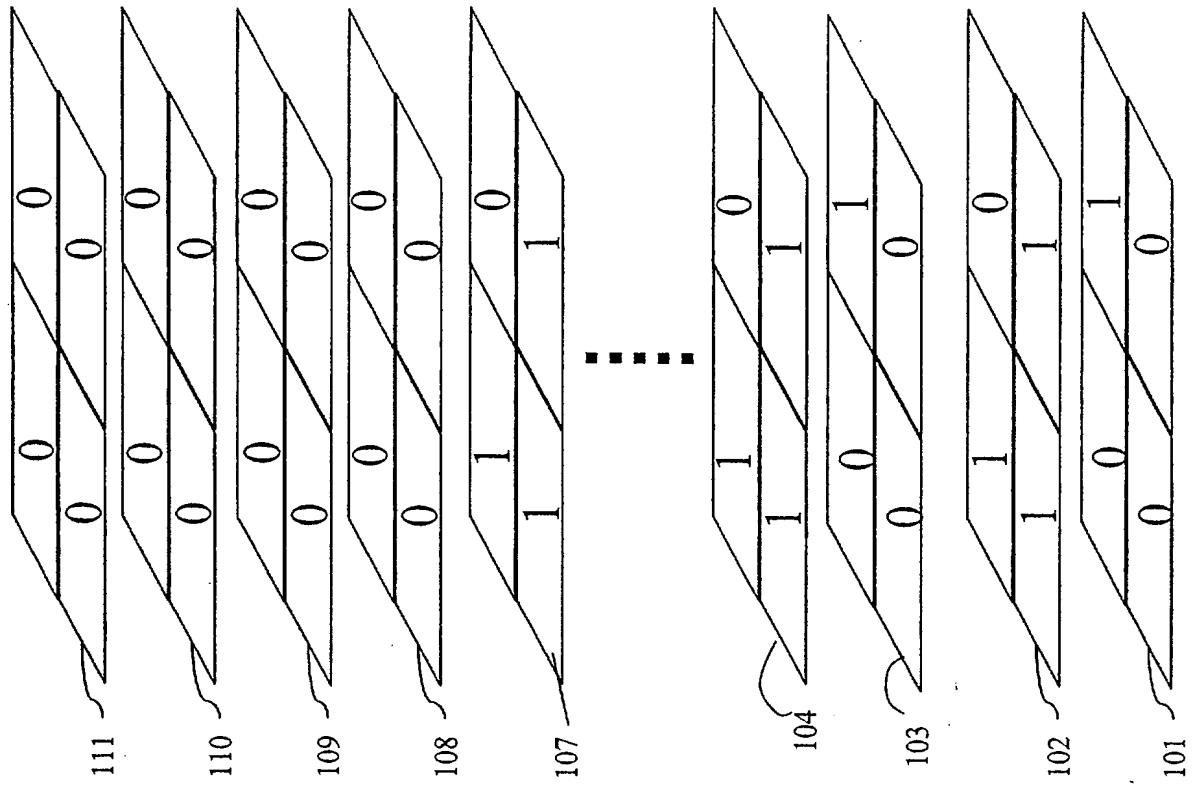


Fig. 3b

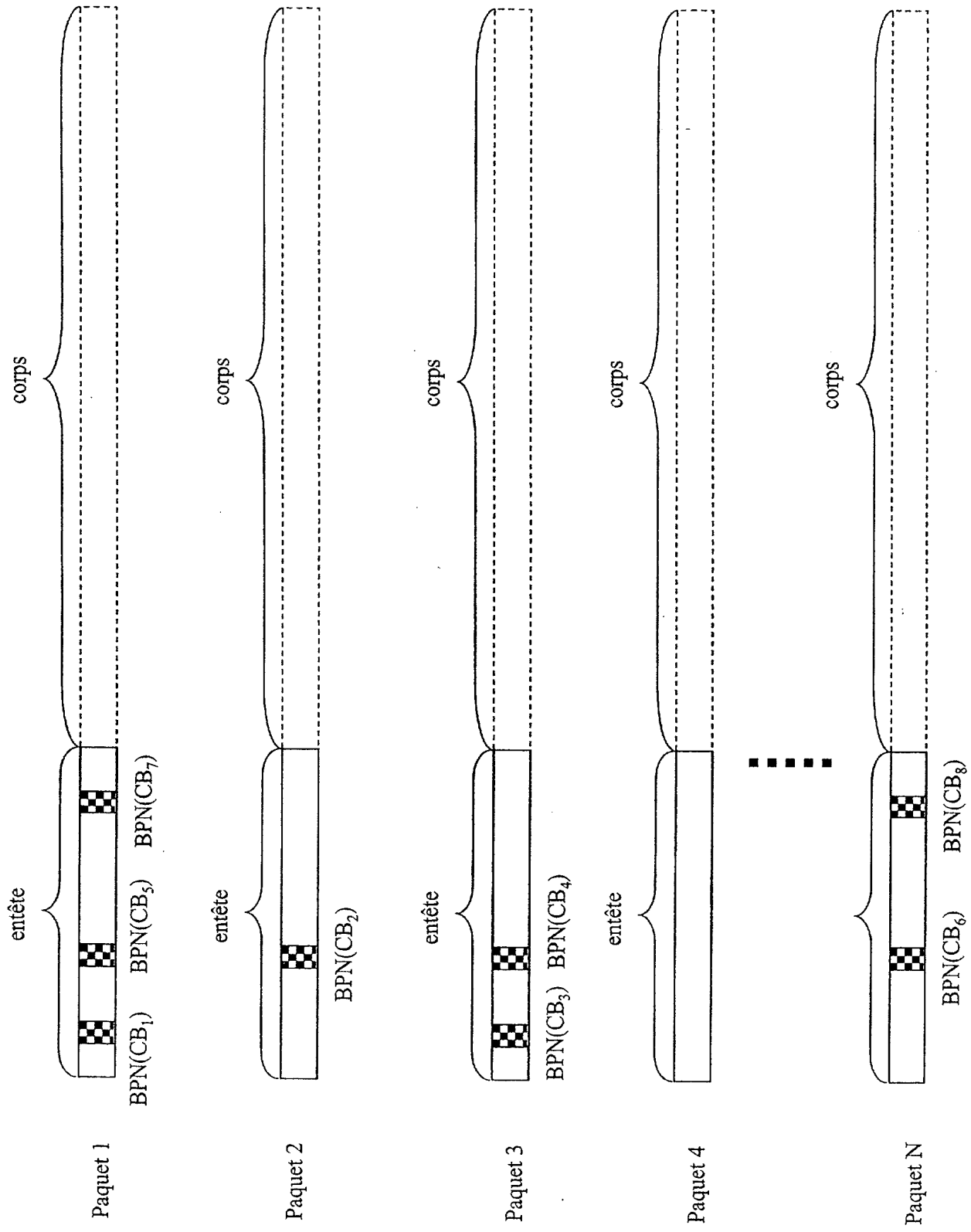


Fig. 4

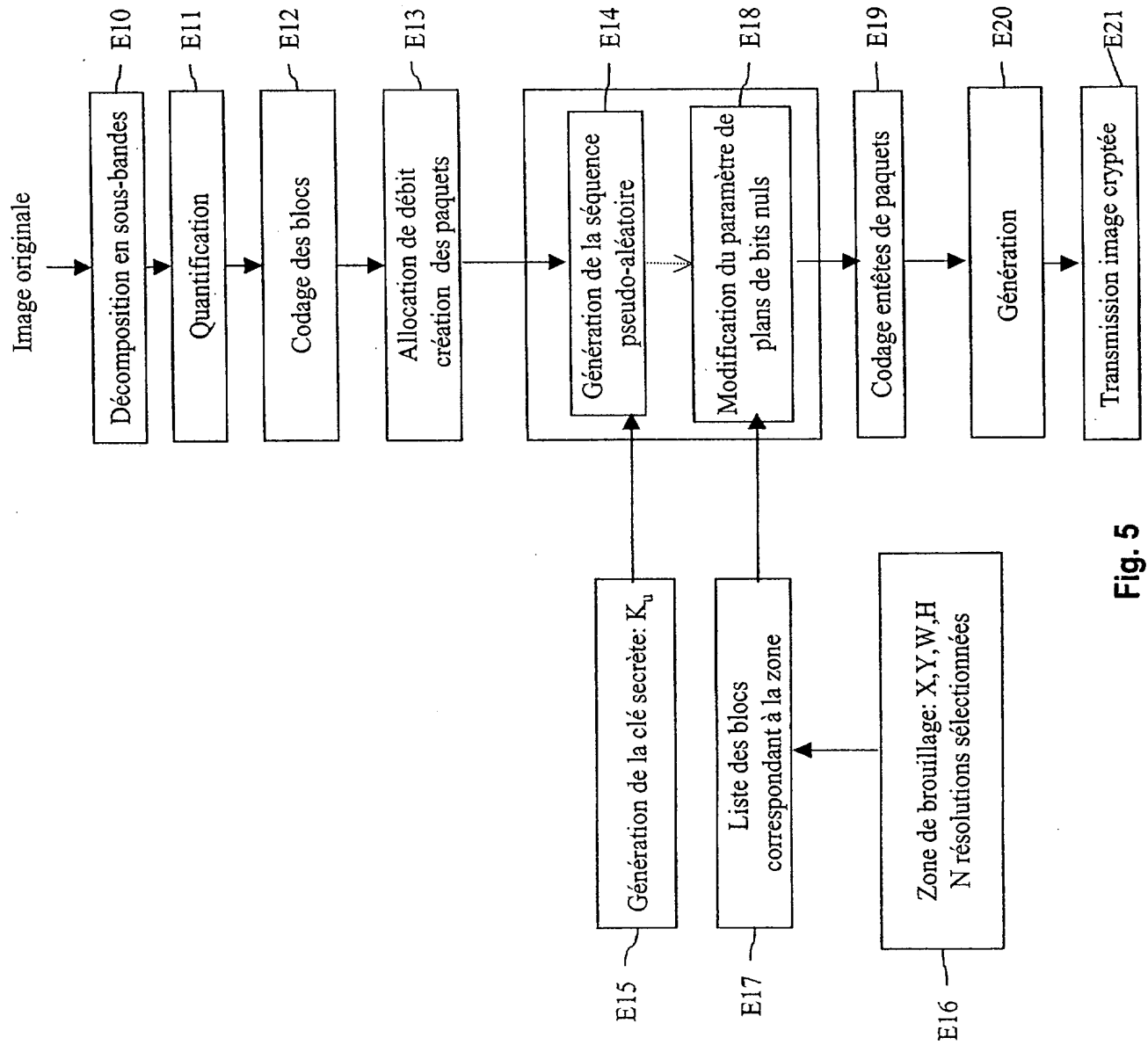


Fig. 5

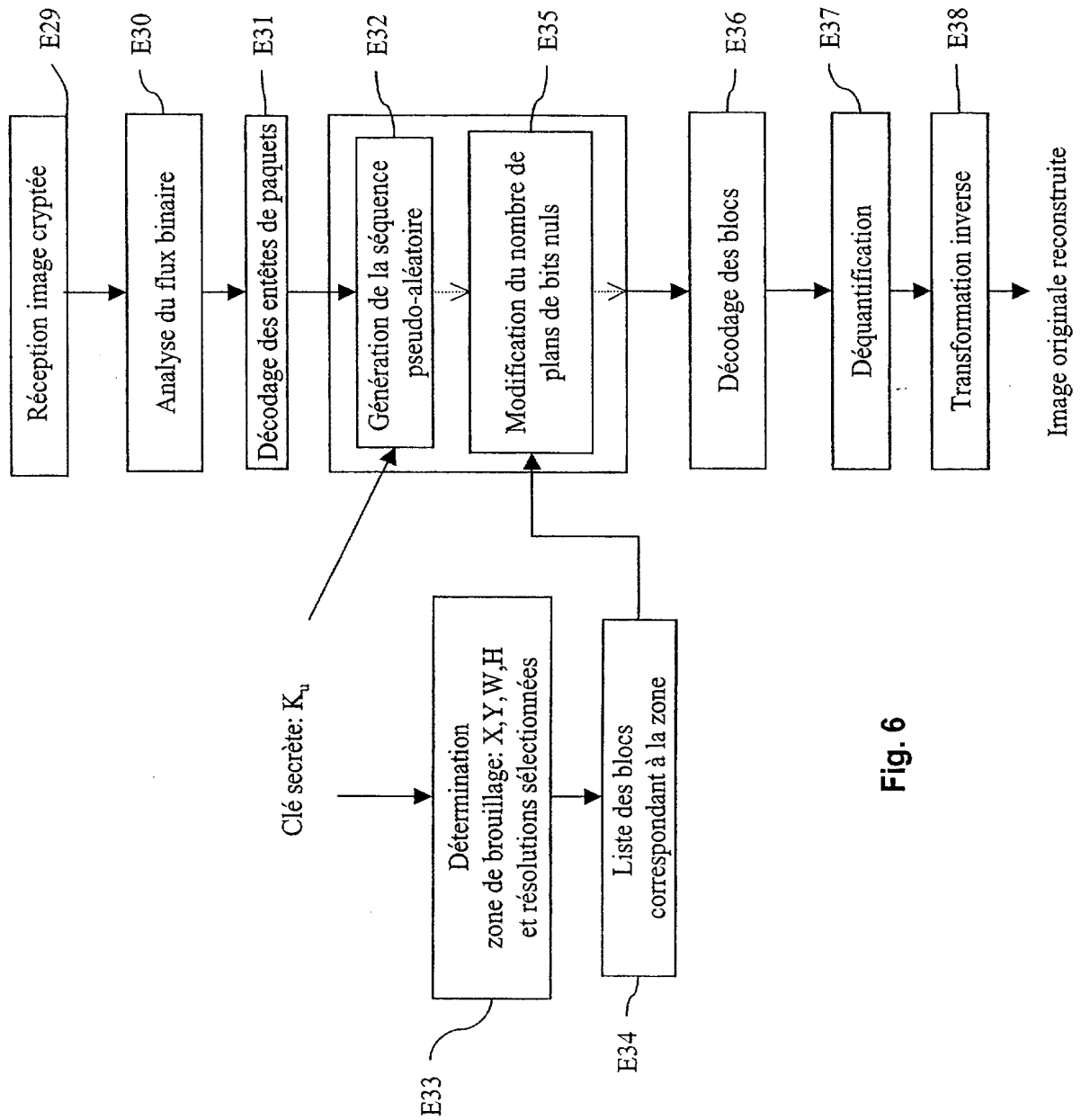


Fig. 6

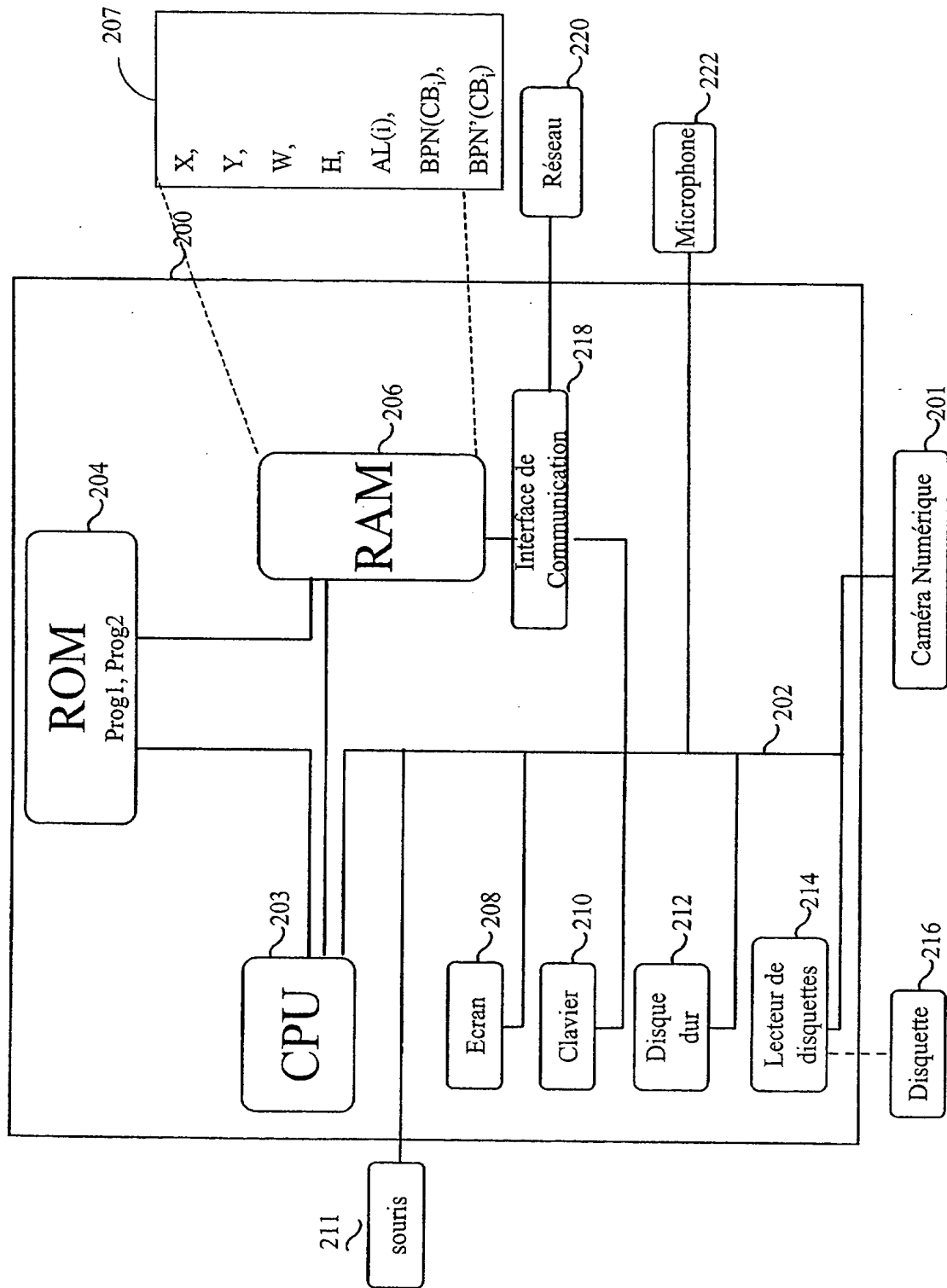


Fig. 7

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1/1

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)



Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 300301

Vos références pour ce dossier (facultatif)		BIF023190/MP/L IH	
N° D'ENREGISTREMENT NATIONAL		0209134	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Procédé et dispositif de transformation d'un signal numérique			
LE(S) DEMANDEUR(S) :			
CANON KABUSHIKI KAISHA			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		ONNO	
Prénoms		Patrice	
Adresse	Rue	60 avenue du Sergent Maginot	
	Code postal et ville	35000 RENNES, France	
Société d'appartenance (facultatif)			
Nom		LE LEANNEC	
Prénoms		Fabrice	
Adresse	Rue	La Gaudais	
	Code postal et ville	35510 CESSON SEVIGNE, France	
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Le 18 juillet 2002 Maxime PETIT N°00.0407 RINUY, SANTARELLI	